

The certification body of TÜV Informationstechnik GmbH hereby awards this certificate to the company

RWE Effizienz GmbH
Freistuhl 7
44137 Dortmund, Germany

to confirm that its online shop

RWE SmartHome Shop

fulfils all requirements of the criteria

**Security Qualification (SQ),
Version 9.0**

of TÜV Informationstechnik GmbH. The requirements are summarized in the appendix to the certificate.

The appendix is part of the certificate and consists of 5 pages.

The certificate is valid only in conjunction with the evaluation report until 2013-03-31.



© 2011 TÜVIT GmbH - Member of TÜV NORD Group

Certificate-Registration-No.:
TUVIT-SQ9541.11

13

Essen, 2011-05-13

Joachim Faulhaber
Deputy Head of Certification Body

TÜV Informationstechnik GmbH
Member of TÜV NORD Group
Langemarckstr. 20
45141 Essen, Germany
www.certuvit.de

Certificate

Certification System

TÜV[®]

The certification body of TÜV Informationstechnik GmbH performs its certification on the basis of the following product certification system:

- German document: "Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH", version 1.0 as of 2010-05-18, TÜViT GmbH

Evaluation report

- German document: "SmartHome-Lösung – Auflagenprüfung – Sicherheitstechnische Qualifizierung (SQ)[®] des RWE SmartHome Webshops der RWE Effizienz GmbH", version 1.1 vom 2011-04-07, TÜViT GmbH
- German document: "SmartHome-Lösung – Sicherheitstechnische Qualifizierung (SQ)[®] des RWE SmartHome Webshops der RWE Effizienz GmbH", Version 1.1 vom 17.01.2011, TÜViT GmbH

Evaluation requirements

- German document: "Sicherheitstechnische Qualifizierung (SQ)[®] der TÜV Informationstechnik GmbH", version 9.0 as of 2006-10-01, TÜViT GmbH
- System-specific security requirements (see below)

Evaluation Target

The target of evaluation is the online shop "RWE SmartHome Shop" at the company RWE Effizienz GmbH. The online shop consists of the web application and the system environment. The RWE SmartHome Shop is the central sales platform for the RWE customers. Examined were exclusively the beyond-mentioned system-specific security requirements on the basis of the SQ[®]. Further properties of the online shop are not target of the certification.

Evaluation Result

- All applicable evaluation requirements for the Security Qualification are fulfilled.
- System-specific security requirements are fulfilled.

System-specific security requirements

The certification is based on the following system-specific security requirements that have been checked in the evaluation.

1 Security functions of the system environment

- The system components of the web application that can be accessed from the Internet do not contain any known exploitable vulnerabilities at the time of the technical examination.
- Administration activities are carried out via trusted paths which protect the integrity and confidentiality of the data. The corresponding interfaces are not accessible from the Internet.
- A logging concept is implemented for the operating systems and the server processes.
- The web application is protected by a firewall installation.

2 Security functions of the web application

- The web application makes use of secure authentication token. These authentication token are checked in a secure way by the web application.
- The web application implements or uses secure session management which is suitable for separating the sessions of the users.

- Effective access controls are in place which prevent unauthorised access to the URL, business functions, data, services and files.
- Validation of the input data is implemented.
- The application makes use of output coding.
- Error handling and logging functionalities of the application are suitable in order to identify security-relevant events (e. g. attempted attacks). They do not reveal any confidential information.
- The application utilises secure settings for HTTP communication, so that data transfer is secure. In addition, the data are transferred via HTTPS connections that are secured by means of SSL/TLS.
- The security configuration of the web application is protected against unauthorised changes.

Summary of the requirements for the Security Qualification (SQ), version 9.0

1 Technical security requirements

Technical security requirements are defined based on recognized criteria, specifications or standards. The technical security requirements are free of internal contradictions and satisfy accepted security requirements.

2 Documentation of the architecture

For the qualification of the IT product and its application environment or of the IT system, appropriate descriptions of all necessary components are available. From these, the mutual utilization relationships and data flows as well as the fulfillment of security requirements can be recognized.

3 User, administration and other operational documents

Suitable manuals for installation, administration and usage are available. These particularly include notes on configuration of necessary system and product components as well as environmental measures and personnel responsibilities which satisfy the security requirements.

4 Security of the components used

All sub-components that implement security functionalities could be classified as trustworthy based on previously performed formal evaluations and/or publicly accessible information.

5 Means of system management

Suitable configuration facilities as well as appropriate monitoring and logging guarantee the secure operational state. Tools used for system management are subject to the same security requirements as the IT product/IT system itself.

6 Tests and inspections

Comprehensive penetration testing and technical vulnerability analyses have been performed during testing. The vulnerabilities determined during testing and analyses have been rated according to their risk potential.

7 Change management

A concept for the planning and implementation of new configurations and the import of updates exist in order to adequately evaluate risks and their effects as well as to guarantee maintenance of the intended protective level. The concept describes the way in which changes may take

place and how the documentation is adapted where necessary.

8 IT systems: operational environment

Suitable operational conditions exist. The personnel responsibilities and environmental conditions satisfy the security claim of the IT system.

9 Security analyses

In a final analysis documented in the evaluation report the results of the previously listed evaluation aspects are compared to the security requirements. The result is that all security requirements have been met and the resulting residual risks are bearable.